वर्गीय अपेक्षाओं के लिए मानक

टीईसी ९१०१०:२०२६

(सं. टीईसी ९१०१०:२०२३ को अधिक्रमित करता है)

STANDARD FOR GENERIC REQUIREMENTS

TEC 91010:2026

(Supersedes No. TEC 91010:2023)

क्वांटम सुरक्षित क्रिप्टोग्राफ़िक प्रणालियाँ

Quantum-Safe Cryptographic Systems

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली- 110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA

www.tec.gov.in

Release 2: May, 2026

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

Quantum-safe cryptographic systems are designed to protect communications and sensitive data against both current and future threats, including those posed by quantum computing. This document

outlines the general requirements and technical specifications for such systems, covering cryptographic modules and their secure design, implementation, operation, and management. Its goal is to establish a unified framework that ensures secure communication, strong data protection, and adaptability (cryptographic agility) as threats evolve.

Additionally, the document defines requirements for vendors to support testing, certification, and compliance evaluation of their products and services. It also provides guidance for organizations to make informed decisions when procuring, deploying, operating, and maintaining secure and interoperable cryptographic solutions.

CONTENTS

HISTORY SHEET

Sl. No.	*Standard/document No.*	*Title*	*Remarks*
1.	TEC 91010:2023	Generic Requirements of Quantum-safe and Classical Cryptographic Systems	First Issue
2.	TEC 91010:2026	Generic Requirements of Quantum-safe Cryptographic Systems	Second Issue

REFERENCES

Sr. No.	*Document No.*	*Title/Document Name*
1.	CISPR 32/ or IS/CISPR 32: 2015	Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment
2.	ETSI TR 103 619 V1.1.1 (2020-07)	Migration strategies and recommendations to Quantum-safe schemes
3.	ETSI GS QKD 014 V1.1.1 (2019-02)	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API
4.	FIPS 140-3	Security Requirements for Cryptographic Modules
5.	FIPS PUB 197	Advanced Encryption Standard (AES) 2001
6.	FIPS PUB 198	The Keyed-Hash Message Authentication Code (HMAC) 2002
7.	IEC 60825-2/ IS 14624-2	Safety of laser products Part 2 safety of optical fibre communication systems OFCS (First Revision)
8.	IEC 61000-4-11/ IS 14700 (Part 4/Sec 11):2020	Testing & measurement technique- voltage dips, short interruptions, and voltage variations immunity tests.
9.	IEC 61000-4-2 / IS 14700 (Part 4/Sec 2): 2018	Testing and measurement techniques of Electrostatic discharge immunity test
10.	IEC 61000-4-29	Testing and measurement techniques- Voltage dips, short interruptions, and voltage variations on D.C input power port immunity test.

11.	IEC 61000-4-3/. IS 14700 (Part 4/Sec 3): 2010	Radiated RF electromagnetic field immunity test
12.	IEC 61000-4-4/ IS 14700 (Part 4/Sec 4): 2018	Testing and measurement techniques of electrical fast transients/burst immunity test
13.	IEC 61000-4-5(2017)/ IS 14700 (Part 4/Sec 5): 2019	Testing & Measurement techniques for surge immunity test.
14.	IEC 61000-4-6 / IS 14700 (Part 4/Sec 6): 2016	Testing & Measurement techniques for surge immunity test and Immunity to conducted disturbances
15.	IEEE 802.1AE	Media Access Control (MAC) Security
16.	IEEESTD.2018.8585421	IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security. IEEE.
17.	IEC 60215/ IS 10437(1986)	Safety requirements for radio transmitting equipment
18.	IEC 60950-1(2005)/ IS 13252 (2010)	Safety of information technology equipment
19.	ISO/IEC 10116:2006 / IS 15116 : 2018	Information technology – Security techniques – Modes of operation for an n-bit block cipher
20.	ISO/IEC 18033-3:2010/	Information Technology Security Techniques Encryption algorithms
21.	ISO/IEC 19790:2025	Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

22.	ISO/IEC 24759:2025	Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules
23.	ITU-T X.1710	Security framework for quantum key distribution networks Series X: Data Networks, Open System Communications And Security
24.	ITU-T X.1810	Framework for quantum-safe cryptography
25.	ITU-T X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems
26.	ITU-T X.1812	Quantum-safe cryptographic mechanisms and applications
27.	ITU-T X.800	Security architecture for Open Systems Interconnection for CCITT applications
28.	ITU-T Y.3802	Quantum key distribution networks - Functional architecture
29.	ITU-T Y.3803	Quantum key distribution networks - Key management
30.	ITU-T Y.3804	Quantum key distribution networks - Control and management
31.	NISTIR 8105	Report on Post-Quantum Cryptography
32.	TEC 11016:2016 (Old No. TEC/SD/DD/EMC -221/05/OCT-16)	Electromagnetic Compatibility Standard for Telecommunication Equipment
33.	TEC 14016:2010 (Old No. QM-333)	Standard for Environmental testing of Telecommunication equipment
34.	RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
35.	RFC 3686	Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP)
36.	RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating

37.	RFC 4301	Security Architecture for the Internet Protocol
38.	RFC 4302	IP Authentication Header
39.	RFC 4303	IP Encapsulating Security Payload
40.	RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
41.	RFC 4308	Cryptographic Suites for IPsec
42.	RFC 4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
43.	RFC 5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange Protocol Version 2 (IKEv2)
44.	RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
45.	RFC 8221	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
46.	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3
47.	RFC 9052	Authoritative specification for CBOR Object Signing and Encryption (COSE) for signing, encryption, and authentication of data objects
48.	RFC 9180	Hybrid Public Key Encryption (HPKE)
49.	RFC 7696	Guidelines for Cryptographic Key Management
50.	RFC 8221	Mandatory Algorithms for DNSSEC
51.	RFC 5751	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification
52.	RFC 4880	OpenPGP Message Format
53.	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
54.	ISO/IEC 15408	Common Criteria for Information Technology Security Evaluation

	(All Parts)	

Note: Unless otherwise explicitly stated, the latest approved issue of the documents referred to above, with all amendments in force, on the issuance date of this GR shall be applicable.

CHAPTER 1

Introduction to Cryptographic Systems

1.1 Introduction to Cryptographic Systems

Cryptography is the practice of securing communication and protecting data from unauthorized access by converting plaintext into ciphertext using mathematical algorithms, making it unintelligible to anyone without the proper key. It plays a critical role in securing our digital infrastructure.

The typical cryptographic system is shown in Figure 1. The original message is usually termed plaintext and the scrambled message is called the ciphertext. The encryption algorithm converts the plaintext to the ciphertext and the decryption algorithm performs a reverse process to get back the original message.

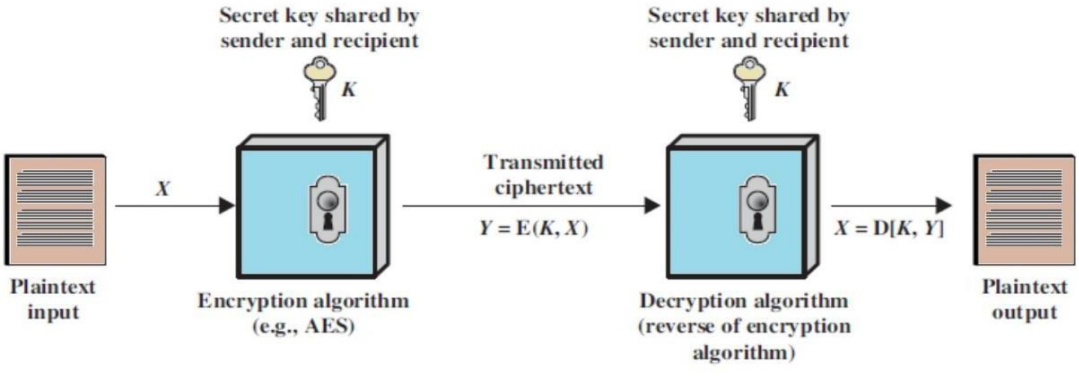

Figure 1: Block Diagram of a typical Cryptographic System

Our most crucial communication protocols rely on three core cryptographic primitives: public key encryption, digital signatures and key exchange. These primitives are implemented using state-of-the-art of cryptographic algorithms, e.g., AES, Diffie-Hellman Key Exchange(DHKE), the RSA (Rivest-Shamir-Adleman) algorithm, and elliptic curve cryptography(ECC).

The security of the public key cryptographic primitives as mentioned above depends on the difficulty of a number of theoretical problems, such as Integer Factorisation and the Discrete Log problem. In 1994, Peter Shor showed that Quantum computers, a new technology leveraging the physical properties of matter and energy to perform calculations, can efficiently solve factorisation and discrete log problems, thereby rendering all public key cryptosystems based on such assumptions insecure. Thus, a sufficiently powerful quantum computer will peril many forms of modern communication, from Key exchange to encryption to digital authentication. As a result, RSA and DHKE are no longer secure in a post-quantum era.

Further, for data encryption, symmetric algorithms such as AES are widely used. Grover's algorithm offers a quadratic speed-up for brute-force key search compared to classical search, therefore, it can affect AES (and other symmetric encryption algorithms) by reducing the effective security of an n-bit key n/2 bit security on a sufficiently powerful quantum computer—so, for example, AES-128 would offer roughly ~64-bit quantum security, which is why doubling the symmetric key length is generally considered necessary to maintain the same security margin against quantum adversaries but not solely sufficient to prevent attack from quantum computer.

Table 1: Impact of Quantum Computing on common cryptographic algorithms

Sl. No.	Cryptographic Algorithm	Type	Purpose	Impact of the large scale quantum computer
1.	AES	Symmetric Key	Encryption	Larger key sizes needed
2.	SHA-2, SHA-3	----------		SHA-2, SHA-3
3.	RSA	Public key	Signatures, key establishment	No longer secure
4.	ECDSA, ECDH	Public key	Signatures, key exchange	No longer secure

Quantum-safe cryptographic systems, also known as post-quantum cryptography, are designed to be resistant to attacks from both classical and quantum computers. These systems use algorithms that are believed to be secure even against quantum computers. Quantum-safe cryptography is becoming increasingly important as quantum computers continue to evolve and become more powerful.

It is, therefore, critical to begin planning the replacement of hardware, software, and services that can interoperate with existing communications protocols and networks. Most quantum-resistant algorithms have larger Key sizes than the ones they will substitute, which is a big challenge. Quantum-safe algorithms may change various Internet protocols, such as the Transport Layer Security (TLS) protocol or the Internet Key Exchange (IKE). Implementing quantum-safe algorithms

requires identifying hardware and software modules, operating systems, communication protocols, cryptographic libraries, and applications employed in data centres on-premises or in the cloud and distributed computing, storage, and network infrastructures. From a compliance and risk-management perspective, transitioning to quantum-safe cryptography helps address long-term confidentiality concerns such as “harvest now, decrypt later,” where encrypted sensitive data captured today could potentially be decrypted in the future if cryptographically relevant quantum capabilities emerge.

1.2 Classification of cryptographic algorithms

Cryptographic algorithms are broadly classified into two categories, traditional and modern, based on the type used during the encryption and decryption process (refer to figure 2).

1.3 Traditional Cryptography

Traditional cryptography refers to cryptographic methods and techniques developed before the advent of computers.

1.4 Modern Cryptography

Modern cryptography is based on publicly known mathematical algorithms that operate on binary bit sequences and utilise secret keys. There are three types of modern cryptography:

i. Symmetric (Secret Key) cryptography
ii. Asymmetric (Public Key) cryptography

iii. Cryptographic Hash Functions

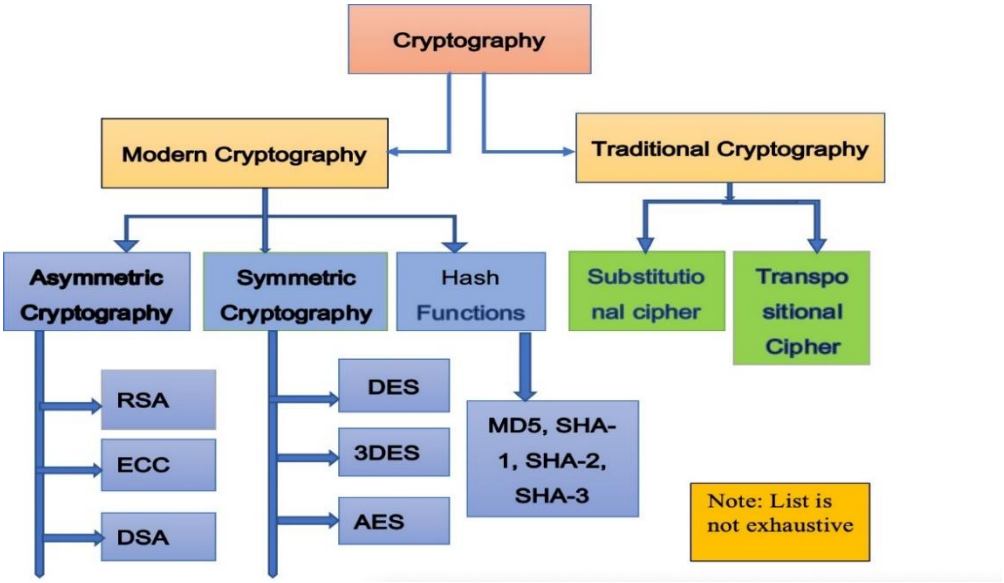

Figure 2: Block Diagram of classification of classical cryptography

1.4.1 Symmetric key cryptography

Encryption and decryption keys are identical in this scheme and should be known only to the communicating parties. Symmetric key cryptography is much faster than Asymmetric key cryptography, is far less resource-intensive than asymmetric encryption and is an incredibly efficient way to protect large volumes of data. Examples are Advanced Triple-Data Encryption Standard (DES), i.e., 3DES, Advanced Encryption System (AES), etc.

1.4.2 Asymmetric Key Cryptography

In this scheme, two keys are used, i.e., public key (for encryption) and private key (for decryption). The private key is kept secret as it is used for decryption, while the public key is not. For a secure public key cryptosystem, it is impossible to determine the private key's value by knowing the corresponding public key.

Most public communication networks use a combination of asymmetric and symmetric key cryptography schemes. An asymmetric/ Public Key

Cryptography scheme is used for key distribution. At the same time, the data flow is secured using a symmetric technique because of its better performance in the encryption/decryption process.

1.4.3 Hash Function

A Hash function is a cryptographic algorithm that takes an input message of any size and outputs a short fingerprint of fixed length. Typically, it does not require any key along with the input message, and the output is usually called hash-value or hash-digest. These algorithms are typically used to ensure the authenticity or integrity of data. Hash functions can also use keys, referred to as Keyed-hash functions, under such usage. Many operating systems/applications store passwords using hash functions.

1.5 Types of configuration of cryptographic system

1.5.1 A cryptographic module shall be a set of hardware, software, firmware or some combination thereof that at a minimum, implements a defined cryptographic service employing an approved cryptographic algorithm, security function or process and contained within a defined cryptographic boundary.

1.5.2 The cryptographic systems can be classified based on the hardware, software and or firmware used in modular form within the cryptogpraphic boundary. These modules may be part of any interdependent or standalone system.

1.5.3 The cryptographic module/system can be defined as one of the following types:

i. Hardware module: It is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within the hardware cryptographic boundary.

ii. Software module: It is a module whose cryptographic boundary delimits the exclusive software component(s) (may be one or multiple software components) that execute(s) in an adjustable operational environment. The computing platform and operating system of the working environment in which the software performs are external to the defined software module boundary.

iii. Firmware module: It is a module whose cryptographic boundary delimits the exclusive firmware component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment in which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.

iv. Hybrid Software module: It is a module whose cryptographic boundary delimits the composite of a software component and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment in which the software executes are external to the defined hybrid software module boundary.

v. Hybrid Firmware module: It is a module whose cryptographic boundary delimits the composite of a firmware component and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment in which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.

1.6 Classification of Quantum-safe cryptography configuration

The Quantum-safe cryptography module can be classified in a similar manner to classical cryptography modules. However, the algorithms will be different, especially for public key infrastructure like public key encryption schemes, key exchange mechanisms, digital signature schemes and hash functions. These algorithms need to resist attacks by quantum computers, and at the same time, they should still be secure against classical computer attacks.

For symmetric key cryptography, doubling the key size can provide some protection against quantum computing attacks, but this is not a complete solution. New search algorithms are being developed for asymmetric key cryptography to resist quantum computing attacks.

1.6.1 Symmetric Cryptography

Symmetric key cryptography is vulnerable to quantum attacks. It is mostly threatened by Grover's algorithm. Unlike the asymmetric encryption algorithms (eg. RSA, etc) which could be completely broken by the Quantum computer; for symmetric algorithms like AES, the best known Grover's algorithm for attacking these encryption algorithms only weakens them. Grover's algorithm decreases the effective key length of a symmetric encryption algorithm by half, so AES-128 has an effective key space of 2^{64} and AES-256 has an effective key space of 2^{128}.

1.6.2 Quantum-safe asymmetric cryptography

Today's most important uses of public key cryptography are for digital signatures and key establishment. Constructing a large-scale quantum computer would render many of these public key cryptosystems insecure. In particular, this includes those based on the difficulty of integer factorisation, such as RSA and those based on the hardness of the discrete logarithm problems. Quantum-safe Cryptography mainly refers to

developing new asymmetric cryptography techniques that use a different class of hard mathematical problems. There are a few popular Quantum-safe cryptographic approaches that have emerged, such as Lattice-based, Code-based, multivariate-based and hash based cryptography. These mathematically hard problems are believed to be secure against classical as well as quantum computers.

1.6.3 Quantum-safe Hash and Signature functions

Cryptographic hash functions are widely used to provide data integrity and to build digital signature schemes. SHA-2 family hash algorithms (e.g., SHA-256 and SHA-512) are generally considered quantum-safe in the sense that no known quantum algorithm (including Shor's) breaks them outright; instead, the main quantum impact is limited to generic speed-ups such as Grover's algorithm. While Grover's algorithm can reduce the complexity of brute-force search, this impact can typically be addressed by selecting appropriately strong hash functions and security parameters.

Hash-based signature schemes are an important class of quantum-safe digital signatures. Basic constructions such as Lamport–Diffie and Winternitz are one-time signature schemes, meaning each private signing key must be used only once. To enable practical use for multiple signatures, these one-time keys are combined using Merkle tree constructions, allowing a single public key to authenticate a large number of signatures, bounded by the size of the tree. A well-known example is the eXtended Merkle Signature Scheme (XMSS), which is a stateful hash-based signature scheme; it requires careful state management to ensure that one-time keys are never reused. Overall, quantum-safe hash and signature mechanisms provide a robust alternative for digital signatures in a post-quantum transition, particularly for long-term integrity and authenticity requirements.

1.7 Elements or Subsystems and Applications of a cryptographic systems

A cryptographic system relies upon two basic components, i.e., an algorithm (or cryptographic methodology) and a cryptography key. Cryptographic subsystems in classical cryptography are the same as in Quantum-safe cryptographic systems except that different algorithms are implemented on hardware (Key sharing methods are different in Quantum Key Distribution (QKD) and Quantum-safe Cryptography). It also consists of software/firmware modules, operating systems, communication protocols, cryptography libraries, and applications deployed in data centres on-premises or in cloud, distributed computing, storage and network infrastructure.

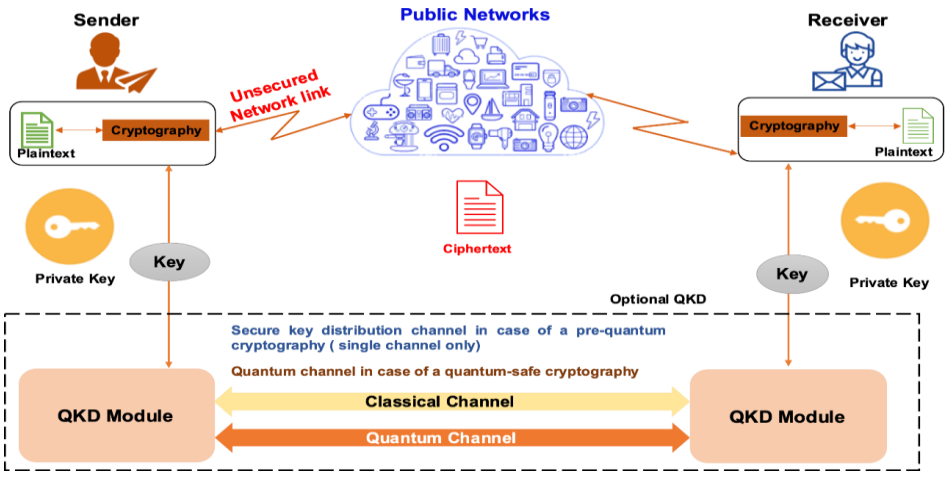

Figure 3: Block Diagram of a Symmetric cryptographic system

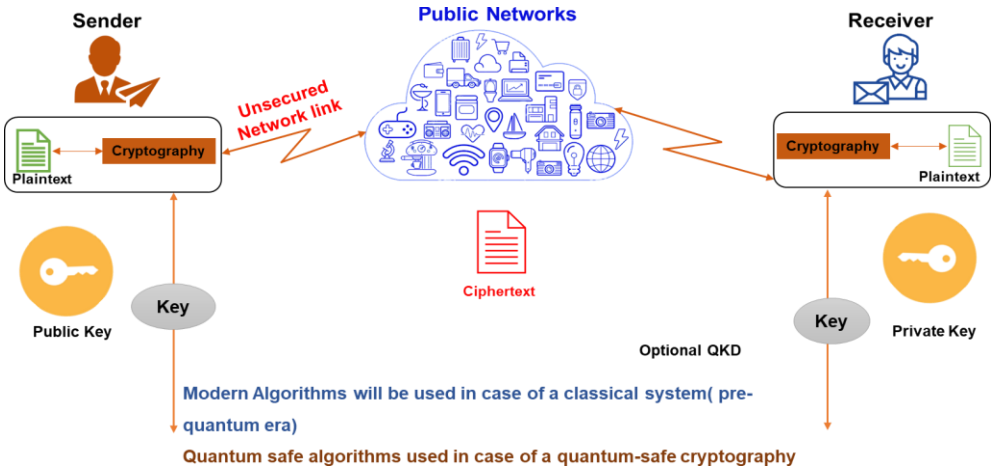

Figure 4: Block Diagram of Asymmetric cryptographic system

QKD, where deployed, may act as an external key source; however, PQC-based mechanisms shall be treated as the primary quantum-safe approach.

Note: Encryption algorithms are the same, but in symmetric cryptographic systems, the key is transported through QKD (if used) is an optional external key source, whereas in the case of Asymmetric cryptography systems, the key is shared using Quantum-safe Cryptography key sharing algorithms. QKD is one of the key sources, as shown in Figure 3.

CHAPTER 2

Functional Requirements

2.1 Core Cryptographic Modules

2.1.1 Cryptographic Processing Module

The Cryptographic Processing Module shall implement the core cryptographic functions required by the system, including one or more functions like encryption, decryption, digital signature generation and verification, hashing, and message authentication. The module shall support hybrid (classical + PQC) or PQC algorithms. Below are the functional requirements of the Cryptographic Processing module applicable as per function supported by module.

2.1.2 The cryptographic processing module shall implement cryptographic processing function including symmetric and asymmetric encryption/decryption, hashing, digital signatures, key agreement and key encapsulation mechanism to ensure confidentiality, integrity, authenticity and non-repudiation of data.

2.1.3 The cryptographic processing module shall ensure correctness of all cryptographic operations such that outputs (e.g., decrypted plaintext, verified signatures, derived shared secrets, hash values) match expected results as defined in the applicable cryptographic standards and test vectors.

2.1.4 The cryptographic processing module shall support only approved cryptographic algorithms, including symmetric, asymmetric, and post-quantum algorithms, and shall reject deprecated or insecure algorithms (e.g., RC4, MD5, DES, SHA-1, ECB mode) and unsupported configurations.

2.1.5 The cryptographic processing module shall support cryptographic keys of approved types and sizes and shall validate all keys to ensure correctness, randomness, and compliance with applicable standards, rejecting invalid or weak keys.

2.1.6 The cryptographic processing module shall implement approved modes of operation and shall avoid legacy or insecure modes unless used with appropriate integrity protection mechanisms. Authenticated encryption modes (e.g., GCM) shall be supported for combined confidentiality and integrity.

2.1.7 The cryptographic processing module shall correctly generate, manage, and use cryptographic parameters such as Initialization Vectors (IVs), nonces, salts, and domain separation values, ensuring randomness, uniqueness, and compliance with the selected algorithm requirements.

2.1.8 The cryptographic processing module shall validate all inputs, including plaintext, ciphertext, messages, keys, signatures, and parameters, and shall handle boundary and edge cases (e.g., empty, null, oversized inputs) securely without causing unintended behavior or security compromise.

2.1.9 The cryptographic processing module shall ensure integrity protection by detecting any tampering or unauthorized modification of ciphertext, messages, or signatures and shall fail securely upon such detection.

2.1.10 The cryptographic processing module shall correctly implement padding schemes, encoding formats, and message structures as defined in applicable standards and shall reject malformed or improperly formatted inputs.

2.1.11 The cryptographic processing module shall support hashing functions compliant with approved standards and shall correctly process inputs of varying sizes, including incremental processing, and shall produce outputs matching known answer test vectors.

2.1.12 The cryptographic processing module may support MAC algorithms (e.g., HMAC, CMAC, KMAC) and shall ensure correct key handling, message processing, and output generation consistent with the underlying hash or block cipher functions.

2.1.13 The cryptographic processing module shall support digital signature generation and verification using approved algorithms and shall ensure that signatures are bound to the message and key, rejecting forged, altered, or invalid signatures.

2.1.14 The cryptographic processing module shall support secure key agreement and key encapsulation mechanisms and shall ensure that derived shared secrets or recovered keys are correct and consistent across communicating entities.

2.1.15 The cryptographic processing module shall ensure non-deterministic behavior where applicable, such that repeated operations (e.g., encryption or signature generation) using the same input and key produce different outputs when required by the algorithm.

2.1.16 The cryptographic processing module shall ensure interoperability such that cryptographic outputs (e.g., ciphertexts, signatures, keys, hashes) generated by one compliant implementation can be successfully processed by another implementation conforming to the same standards.

2.1.17 The cryptographic processing module shall implement secure error handling and shall reject invalid inputs, malformed data, unsupported parameters, and unauthorized operations without exposing sensitive information.

2.1.18 The cryptographic processing module shall implement protections against side-channel attacks, including timing and memory-based leakage, as applicable to the implementation environment.

2.1.19 The cryptographic processing module shall securely erase cryptographic keys, intermediate values, and sensitive data from memory after use to prevent residual data exposure.

2.1.20 The cryptographic processing module shall operate within defined performance limits for all supported cryptographic operations under specified operating conditions and shall be suitable for the intended deployment environment.

2.1.21 The module shall support secure key agreement classical mechanisms (e.g., Diffie–Hellman, Elliptic Curve Diffie–Hellman Ephemeral) and post quantum key encapsulation and digital signature mechanisms (e.g., ML-KEM, ML-DSA, SLH-DSA, FN-DSA, HQC) including post-quantum hybrid schemes (e.g., X25519 + ML-KEM), ensuring correct operations.

2.1.22 The cryptographic module shall provide mechanisms for cryptographic agility, including the ability to enable, disable, or restrict the use of algorithms, modes, and key sizes through configuration or policy control. The module shall support deprecation of insecure or obsolete algorithms without requiring system redesign.

2.1.23 The module shall enforce minimum key sizes as per applicable security strength requirements (e.g., AES ≥ 128-bit, RSA ≥ 2048-bit, ECC ≥ 224-bit or equivalent).

2.2 Hybrid Cryptographic Schemes (Classical + PQC)

i. The cryptographic module shall ensure that hybrid constructions correctly combine classical and post-quantum components using approved composition methods (e.g., concatenation followed by key derivation function).

ii. The cryptographic module shall ensure that the overall security of the hybrid scheme is not weaker than the strongest individual component and that no downgrade or fallback to weaker algorithms is permitted.

iii. The cryptographic module shall validate that both classical and PQC components independently satisfy their respective algorithmic correctness and security requirements.

iv. The cryptographic module shall ensure interoperability of hybrid schemes across compliant implementations and shall correctly process hybrid keys, ciphertexts, and signatures.

v. The cryptographic module shall provide documented procedures for validation, verification, and testing of hybrid cryptographic operations.

2.3 Post-Quantum Cryptographic Algorithm Verification

2.3.1 General Algorithm Validation

i. The cryptographic module shall validate post-quantum cryptographic algorithms against officially published parameter sets, ensuring that all domain parameters, key sizes, and internal constants conform to the applicable algorithm specifications.

ii. The cryptographic module shall demonstrate conformance to official Known Answer Tests (KAT), test vectors, and reference implementations for all supported PQC algorithms.

iii. The cryptographic module shall ensure that implementations do not use reduced or non-standard parameter sets that weaken the intended security level.

iv. The cryptographic module shall ensure that all probabilistic components of PQC algorithms (e.g., noise sampling, randomness

generation, rejection sampling) follow the statistical distributions and properties defined in the respective algorithm specifications.

2.3.2 Code- Based Cryptographic Algorithms

i. The cryptographic module shall ensure that code-based schemes correctly implement encoding and decoding operations based on the underlying error-correcting codes (e.g., Goppa codes, quasi-cyclic codes) as defined in the algorithm specification.

ii. The cryptographic module shall ensure that error vectors are generated with the correct weight and distribution and that decoding operations correctly recover the original message or shared secret.

iii. The cryptographic module shall validate that ciphertexts and public keys conform to the required algebraic structure and size constraints defined in the scheme.

2.3.3 Lattice-Based Cryptographic Algorithms (LWE / R-LWE)

i. The cryptographic module shall ensure that polynomial arithmetic (e.g., modular reduction, Number Theoretic Transform (NTT), inverse NTT) is implemented correctly and consistently across all operations.

ii. The cryptographic module shall validate that ciphertexts and keys satisfy the underlying LWE/R-LWE mathematical relations and that decryption correctness holds within defined error bounds.

iii. The cryptographic module shall ensure that parameter sets (e.g., modulus, dimension, noise bounds) meet the required security level and are not weakened in implementation.

iv. The cryptographic module shall ensure correct implementation of noise sampling mechanisms (e.g., discrete Gaussian or centered

binomial distribution) and shall verify that sampled values conform to the required statistical distribution.

v. The cryptographic module shall ensure that decryption failure probability remains within the bounds specified by the algorithm and that implementation does not introduce increased failure rates.

2.3.4 Hash-Based Cryptographic Algorithms

i. The cryptographic module shall ensure correct implementation of hash-based constructions, including one-time signatures and tree-based structures (e.g., Merkle trees, XMSS, SPHINCS+), as defined in the applicable specifications.

ii. The cryptographic module shall ensure that internal state management (e.g., leaf index, tree traversal) is correctly maintained and that state reuse or duplication is prevented.

iii. The cryptographic module shall ensure correct use of domain separation and hash function inputs to avoid cross-protocol or cross-instance collisions.

2.3.5 Post-Quantum Digital Signature Algorithms

i. The cryptographic module shall ensure that signature generation correctly incorporates randomness or deterministic processes as defined in the algorithm specification and shall prevent reuse of secret-dependent values across signatures.

ii. The cryptographic module shall ensure that signature verification correctly validates all mathematical conditions defined in the algorithm, including bounds checking and rejection conditions.

iii. The cryptographic module shall ensure that generated signatures conform to specified encoding formats and size constraints as defined in the applicable standard.

Note-

1. *The testing of classical cryptographic algorithms is out of the scope of this GR and for classical algorithms, the vendor may submit already available test certificate or declaration.*
2. *For post quantum algorithmic validation, Test certificates issued under Cryptographic Algorithm Validation Program (CAVP) or equivalent validation programs shall be acceptable.*

2.4 Random Number Generator Module

In cryptography, randomness is found everywhere, from the generation of keys to encryption systems, even how cryptosystems are attacked. Without randomness, all crypto operations would be predictable and hence, insecure. A good random number generator consists of two parts: a source of entropy and a cryptographic algorithm. Cryptographic algorithms require Keys. A Random Number Generator (RNG), also called a Random Bit Generator (RBG), is needed in the key generation process to create a random (strong) key as well as for other cryptographic purposes such as initialisation vectors and nonces. Typically, a True Random Number Generator (TRNG) provides a source of randomness or “entropy” to seed a Pseudo-Random Number Generation (PRNG), also called a Deterministic Random Bit Generator (DRBG).

Random bit generation	ISO/IEC 18031 OR TEC GR QRNG TEC 91020:2024 Test Guide of GR QRNG TEC 91021:2024 OR	Developers must demonstrate that their entropy source is sufficiently random through a combination of design and/or test processes and

	NIST SP 800-90 Series	continuous checks during operation for any fault that could have catastrophic consequences for generating secure cryptographic keys.

2.5 Key Management Module

Deals with generating keys, verifying keys, exchanging keys, storing keys, and at the end of their lifetime, destroying keys. The bigger the key, the more secure the algorithm will be. The only negative of having an extremely long key is that the longer the key, the more the CPU is used to decrypt and encrypt data.

Below are the functional requirements for key management module –

2.5.1 The key management module shall support secure generation of cryptographic keys, including asymmetric and/or symmetric and where applicable post-quantum keys, using approved mechanisms ensuring sufficient entropy, correct key sizes, and compliance with defined algorithm specifications.

2.5.2 The key management module shall ensure secure storage and protection of cryptographic keys within a defined boundary, maintaining confidentiality and integrity, and shall support secure key wrapping and unwrapping mechanisms using approved cryptographic methods.

2.5.3 If the key management module supports distribution or exchange of cryptographic keys, such operations shall be performed through approved mechanisms. Keys transmitted via in-band or out-of-band methods shall be protected against unauthorized access, disclosure, and modification.

Keys designated as non-exportable shall not be distributed outside their cryptographic boundary.

2.5.4 The key management module shall enforce controlled usage of cryptographic keys in accordance with defined policies and attributes, ensuring that keys are used only for their intended purposes such as encryption, decryption, signing, or verification.

2.5.5 The key management module shall support complete key lifecycle management including generation, activation, suspension, revocation, expiration, archival, and secure destruction, ensuring that invalid or expired keys are not used for any cryptographic operation.

2.5.6 The key management module shall provide secure mechanisms for backup and recovery of cryptographic keys, ensuring preservation of confidentiality and integrity and enabling restoration of keys without loss of functionality or security.

2.5.7 The key management module shall support secure import and export of cryptographic keys in standardized formats, ensuring integrity, authenticity, and protection of keys during transfer across systems.

2.5.8 The key management module shall support interoperability with external systems through standardized protocols such as KMIP, ensuring consistent handling of key formats, attributes, and metadata.

2.5.9 The key management module shall enforce key attributes and policy controls, including usage restrictions, access control, and lifecycle parameters such as activation and expiration time.

2.5.10 The key management module shall ensure protection against unauthorized access, key extraction, and leakage, and shall implement safeguards against side-channel and fault-based attacks during all key management operations.

2.5.11 The key management module shall provide appropriate error handling by detecting and rejecting invalid, corrupted, or unauthorized key operations

and ensuring that no sensitive information is disclosed through error responses.

2.5.12 The key management module shall perform all key management operations within acceptable performance limits and shall support scalability to handle required volumes of key operations under normal and peak load conditions.

2.5.13 The key management module, where interoperating with external systems, shall support the KMIP for standardized communication between key management systems and client applications, ensuring secure and interoperable key lifecycle operations.

2.5.14 The key management module shall support KMIP operations including key creation, registration, retrieval, update, revocation, and destruction, and shall ensure correct handling of key attributes, metadata, and lifecycle states in accordance with KMIP specifications.

2.5.15 The key management module shall ensure secure communication over KMIP interfaces, including authentication, authorization, and protection of data in transit, and shall prevent unauthorized access or manipulation of cryptographic keys through KMIP transactions.

2.6 Cryptographic Interface and APIs

2.6.1 The cryptographic interface and API module shall provide standardized and secure interfaces for accessing cryptographic services exposed by the cryptographic system. The module shall support widely adopted cryptographic interface standards and frameworks such as PKCS#11, Cryptography API: Next Generation (CNG), Java Cryptography Extension (JCE), and Web Cryptography APIs, as applicable. Where key delivery through QKD system is implemented, the module shall support standardized interfaces aligned with ETSI specifications for QKD key delivery.

2.6.2 The module shall support abstraction of underlying cryptographic implementations such that applications invoking the APIs are independent of specific algorithms, providers, or hardware implementations.

2.6.3 The module shall support dynamic selection and configuration of cryptographic algorithms, providers, and parameters through interfaces without requiring changes to application logic.

2.6.4 The module shall enforce authentication and authorization mechanisms to ensure that only authorized entities can access cryptographic services.

2.6.5 The module shall support secure session or context management for invoking cryptographic operations, including establishment, maintenance, and termination of sessions.

2.6.6 The module shall validate all inputs received through interfaces, including parameters, identifiers, and data structures, and shall reject malformed or unauthorized requests.

2.6.7 The module shall ensure that sensitive information, including cryptographic keys and intermediate data, is not exposed through APIs, logs, error messages, or debug interfaces.

2.6.8 The module shall support integration with both software-based and hardware-backed cryptographic providers through unified interfaces.

2.6.9 The module may support remote invocation of cryptographic services, ensuring confidentiality, integrity, and authentication of data in transit.

2.6.10 The module shall support cryptographic agility at the interface level by enabling addition, removal, or modification of cryptographic algorithms and providers without requiring redesign of the interface.

2.7 Protocol/Application Layer Requirements

2.7.1 General Requirements

2.7.1.1 The system shall implement secure communication protocols at the different TCP layers in compliance with applicable IETF standards and specifications.

2.7.1.2 The system shall support cryptographic negotiation mechanisms within protocols to enable selection of approved algorithms, including post-quantum, and hybrid cryptographic schemes.

2.7.1.3 The system shall ensure interoperability with other compliant implementations of applicable protocols.

2.7.1.4 The system shall prevent downgrade attacks by ensuring that negotiation mechanisms do not allow fallback to insecure or deprecated algorithms.

2.7.1.5 The system shall support integration of post-quantum cryptographic mechanisms and hybrid schemes in accordance with applicable standards and evolving specifications.

2.7.1.6 Where applicable, the system may support integration of externally generated keying material through Quantum Key Distribution (QKD), into protocol operations.

2.7.1.7 The system shall support only secure and up-to-date versions of communication protocols and shall disable by default deprecated or insecure protocol versions.

2.7.1.8 The system shall conform to applicable published RFCs or stable draft specifications for supported protocols and shall ensure correctness of message formats, negotiation procedures, and state transitions.

2.8 X.509 / PKI Requirements

2.8.1 The system shall support X.509 certificates for authentication and shall correctly process certificate structures, extensions, and encoding formats.

2.8.2 The system shall support hybrid or PQC certificates and shall correctly associate algorithm identifiers and parameters.

2.8.3 The system shall support verification of both classical and post-quantum signatures within hybrid certificates.

2.8.4 The system shall support certificate chain validation including mixed algorithm chains and shall ensure trust path correctness.

2.8.5 The system shall ensure compatibility and interoperability of certificates across different systems and implementations.

2.8.6 The system shall ensure that certificate validation mechanisms are resistant to downgrade, truncation, and substitution attacks.

2.8.7 The system shall correctly process and validate algorithm identifiers (OIDs) and encoding formats for both hybrid and post-quantum cryptographic algorithms.

2.9 IKEv2 / VPN Requirements

2.9.1 The system shall implement Internet Key Exchange version 2 (IKEv2) for establishment of secure security associations.

2.9.2 The system shall support secure key exchange mechanisms providing Perfect Forward Secrecy, including post-quantum, and hybrid methods.

2.9.3 The system shall ensure that negotiated session keys are correctly derived and consistent across communicating entities.

2.9.4 The system shall support hybrid key exchange mechanisms combining classical and post-quantum algorithms.

2.9.5 The system shall prevent downgrade to insecure or deprecated key exchange, authentication, or cryptographic algorithms.

2.9.6 The system shall ensure interoperability with other compliant IKEv2 implementations.

2.10 TLS Requirements

2.10.1 The system shall implement Transport Layer Security protocols (with TLS 1.3) supporting secure communication for applications.

2.10.2 The system shall support cipher suite negotiation enabling selection of approved cryptographic algorithms.

2.10.3 The system shall support hybrid key exchange mechanisms combining classical and post-quantum algorithms.

2.10.4 The system shall support integration of post-quantum or hybrid certificates and signatures within protocol handshakes.

2.10.5 The system shall ensure resistance to downgrade attacks and shall prevent fallback to insecure algorithms.

2.10.6 The system shall ensure interoperability across different compliant TLS implementations.

2.10.7 The system shall ensure correct implementation of handshake protocols, including key exchange, authentication, and session key derivation.

2.11 S/MIME Requirements

2.11.1 The system shall support secure email communication using S/MIME protocols for encryption and digital signatures.

2.11.2 The system shall support integration of post-quantum cryptographic mechanisms for key exchange and digital signatures.

2.11.3 The system shall ensure confidentiality, integrity, authentication, and non-repudiation of email communications.

2.11.4 The system shall ensure interoperability with other compliant S/MIME implementations.

2.12 SSH Requirements

2.12.1 The system shall implement Secure Shell (SSH) protocol for secure remote access and communication.

2.12.2 The system shall support secure key exchange mechanisms providing Perfect Forward Secrecy, including post-quantum or hybrid approaches.

2.12.3 The system shall support quantum-safe or hybrid authentication mechanisms for host and user authentication.

2.12.4 The system shall prevent downgrade to insecure or deprecated authentication and key exchange mechanisms.

2.12.5 The system shall ensure interoperability with other compliant SSH implementations.

2.13 Crypto Agility

Crypto agility is the capability of a system, organisation, or infrastructure to rapidly and securely adapt its cryptographic mechanisms—including algorithms, parameters, keys, certificates, and protocols—without requiring major architectural redesign or service disruption. It enables the seamless introduction of new cryptographic algorithms, the coexistence of classical and post-quantum mechanisms (including hybrid constructions), and the timely retirement of deprecated or vulnerable algorithms in response to evolving threats, standards, or regulatory requirements. Crypto agility is a foundational requirement for post-quantum readiness, ensuring that cryptographic transitions can be managed as a controlled, repeatable lifecycle process rather than as disruptive one-time migrations.

2.13.1 Cryptographic Agility Requirements

The below cryptographic agility capabilities can be vendor and product-dependent. For example, a product may support cryptographic switching/configuration but may not support cryptographic negotiation.

i. The system shall support cryptographic agility, enabling the addition, replacement, or deprecation of cryptographic algorithms with minimal architectural redesign.

ii. The system should support algorithm negotiation mechanisms covering hybrid, and quantum-safe cryptographic algorithms.

iii. Cryptographic policies should be externally configurable (e.g., config file, API, or centralized policy server) and shall be protected against unauthorized modification (integrity protection + access control + audit logging).

iv. The system shall support hybrid key establishment mechanisms that combine approved classical cryptographic algorithms with post-quantum cryptographic mechanisms.

v. Hybrid key derivation mechanisms shall ensure cryptographic independence between classical and post-quantum components, such that compromise of one does not affect the security of the other. Forward secrecy should be preserved during hybrid operation, ensuring protection of past session keys even if long-term keys are compromised.

vi. Secure transport mechanisms should use TLS version 1.3 or higher with support for post-quantum cryptography-capable extensions. Legacy and insecure protocols shall be disabled by default.

vii. Protocol downgrade attacks shall be prevented through appropriate cryptographic and protocol-level safeguards.

viii. The system shall support hybrid certificates that enable the use of both classical and post-quantum public keys and digital signatures. Certificate path validation shall function correctly for certificates employing hybrid and post-quantum cryptographic signatures.

ix. The system should support post-quantum cryptographic mechanisms in COSE-based environments, particularly for IoT, embedded systems, and deep packet inspection (DPI) use cases.

x. The performance impact and resource utilization implications of post-quantum cryptographic mechanisms should be documented and optimized.

2.14 Requirements for Constrained devices (Lightweight Cryptography)

The security of resource-constrained devices is critical for eg. in the IoT field, given that everything is interconnected. The concern is that the limited resources on these devices may cause performance issues when

the standard cryptographic algorithms are running on them. Therefore, in recent years, researchers have been working on developing lightweight cryptography and various efficient cryptographic technologies. Its requirements are constrained by security, low cost and high performance.

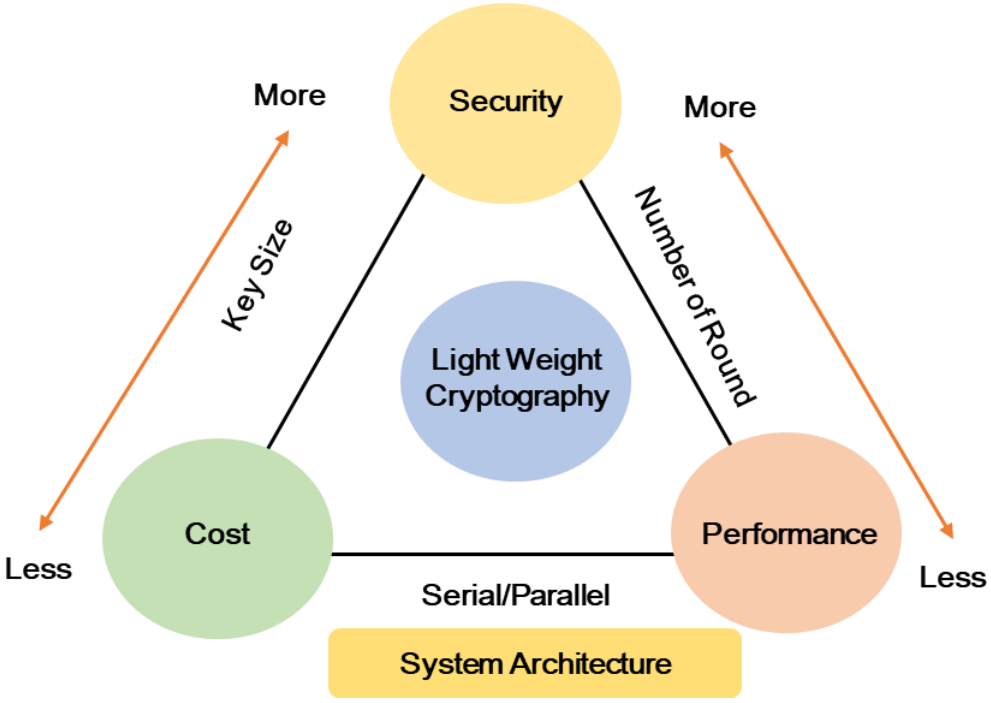

Figure 7: Block Diagram of Lightweight cryptography design trade-offs.

These requirements are balanced accordingly by adjusting the key size, the number of encryption rounds and the system architecture. Thus, the target of lightweight cryptography is to find a better balance between performance and security within cost constraints (refer Figure 7). The chosen algorithms are designed to protect information created and transmitted by the Internet of Things (IoT), including its myriad of tiny sensors and actuators. They are also designed for other miniature technologies, such as implanted medical devices, stress detectors inside roads and bridges, and keyless entry fobs for vehicles.

Devices like these need “lightweight cryptography” protection that uses the limited amount of electronic resources they possess.

The most important in lightweight cryptography: authenticated encryption with associated data (AEAD) and hashing.

AEAD protects the confidentiality of a message, but it also allows extra information, such as the header of a message, or a device's IP address, to be included without being encrypted. The algorithm ensures that all of the protected data is authentic and has not changed in transit. AEAD can be used in vehicle-to-vehicle communications, and it also can help prevent the counterfeiting of messages exchanged with the Radio Frequency Identification (RFID) tags that often help track packages in warehouses. They need to compliant NIST protocols as listed from time to time as per the user requirements.

Sl. No.	Test Category	Description	Expected outcome
1.	AEAD Functionality	Verify AEAD encryption and decryption with associated data (e.g., header)	Data and associated data are encrypted and authenticated correctly
2.	Confidentiality	Ensure message confidentiality over noisy IoT channel using AEAD	Encrypted data not recoverable by unauthorized parties
3.	Authenticity	Test integrity verification when associated data is tampered with	Verification fails, rejecting tampered messages

4.	Key Size Trade-off	Evaluate security vs performance by adjusting key sizes	Smaller keys increase speed but maintain acceptable security levels
5.	Resistance to Attacks	Simulate side-channel and fault injection attacks on AEAD	System withstands attacks without key leakage or authentication bypass
6.	Performance	Measure encryption/decryption speed and power consumption on IoT hardware	Cryptosystem completes operations within device constraints
7.	Compliance Testing	Confirm compliance with NIST Lightweight Cryptography guidelines	Algorithm passes all mandatory compliance tests

In addition to AEAD and hashing, constrained IoT deployments often require digital signatures for firmware authenticity, secure boot / measured boot attestations, device identity, and non-repudiation in audit logs. FN-DSA or FIPS-206 is a digital signature algorithm that can be used for digital signature requirement for constraint devices.

Sl. No.	**Test Category**	**Description**	**Expected outcome**
1.	Signature Functionality	Generate signature and verify signature over representative IoT	Valid signatures verify; invalid signatures fail

		messages (telemetry, control commands)	
2.	Message/Context Binding	Verify signatures bind to correct context (device ID, protocol header, domain separation tag if used)	Replay across contexts fails; correct context verifies
3.	Negative Testing	Verify behavior for modified message, modified signature, wrong public key, truncated inputs	Verification fails reliably without crashes
4.	Key Generation	Test key-pair generation across supported parameter sets; verify key validity checks	Keys generated correctly; invalid keys rejected
5.	Robustness (Malformed Inputs)	Feed malformed/edge-case encodings (oversized, invalid length, non-canonical forms)	Implementation rejects safely; no memory errors
6.	Side-channel Resistance	Evaluate timing/power	No exploitable leakage beyond

		leakage under typical signing and verify operations (where applicable)	acceptable threshold
7.	Fault Injection Resilience	Simulate fault conditions during signing/verification (glitches, bit flips)	No key leakage; faulty signatures do not verify
8.	Performance on IoT HW	Measure sign/verify time, RAM/Flash footprint, and energy consumption	Operations within device constraints; meets procurement limits
9.	Interoperability	Interop test with a known-good reference implementation across parameter sets	Cross-implementation verification succeeds
10.	Compliance Testing	Confirm compliance with applicable NIST/IETF profiles and test vectors	Passes mandatory vectors and profile requirements

Further, ASCON is a lightweight cryptographic family designed for constrained devices and selected by NIST for lightweight cryptography. For IoT, ASCON AEAD provides confidentiality + integrity with associated

data (headers, addresses, counters), while ASCON-Hash supports integrity checks, commitments, and protocol hashing needs.

Sl. No.	Test Category	Description	Expected outcome
1.	Algorithm ID / Variant	Verify the implementation supports the intended standardized functions: Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128, Ascon-CXOF128 (as applicable).	Implemented variants match the claimed functions; unsupported variants are not claimed.
2.	AEAD Correctness	Verify ASCON AEAD encrypt/decrypt with associated data using official test vectors	Ciphertext and tags match vectors; decrypt recovers plaintext
3.	Associated Data Integrity	Modify AD (header/IP/metadata) and verify tag failure	Verification fails; plaintext not released
4.	Nonce Handling	Verify unique-nonce requirement enforcement (generation/storage/anti-reuse)	No nonce reuse in normal operation; reuse detected/mitigated per policy
5.	Tag Verification Behavior	Ensure constant-time tag verification and “fail closed” behavior	No timing oracle; invalid tags always rejected
6.	Misuse / Edge Cases	Test zero-length plaintext/AD, maximum	Correct outputs; no crashes; consistent

		lengths, fragmented inputs	streaming behavior if supported
7.	Replay Protection Support	Validate integration with counters/timestamps as AD (where protocol uses it)	Replayed messages detected by system logic; crypto validates binding
8.	Hash Correctness	Verify ASCON-Hash outputs for standard vectors and typical IoT payloads	Hash outputs match vectors; stable across platforms
9.	XOF Functional Correctness	Validate Ascon-XOF128 supports selectable output length L > 0, correct number of squeezed blocks and correct IV usage.	Output length equals requested L; output matches known-good implementation for various L.
10.	CXOF Customization Handling	Validate Ascon-CXOF128: customization string input Z is supported and incorporated as specified; verify the length constraint	--
11.	Robustness (Malformed Inputs)	Corrupt lengths/encodings and provide malformed buffers	Implementation rejects safely; no memory corruption
12.	Side-channel Resistance	Timing/power analysis on encryption/decryption and hashing (if required)	Leakage within acceptable limits; masking/constant-time validated

13.	Performance on IoT HW	Measure throughput, latency, RAM/Flash, and power on target MCU/SoC	Meets device constraints and procurement targets
14.	Compliance Testing	Confirm conformance to NIST LWC ASCON specifications and published vectors	Passes all mandatory compliance tests

2.15 Cloud based PQC products (Cryptography –as – a- service)

Cloud services have become ubiquitous due to the rise of high-capacity networks, the decreased cost of computers and data storage devices, and trends toward hardware virtualisation and infrastructure, platform, and software-as-a-service models.

2.15.1 Cryptography-as-a-Service

Deploying cryptographic keys to endpoints such as smartphones, virtual machines in the public cloud and smart grid equipment is risky. Therefore, this proposes a Cryptography as a Service (CaaS) model, which allows cryptographic operations to be performed without exposing cryptographic keys and recommends overcoming the pitfalls associated with this technology. Keyed cryptographic operations, such as encryption and decryption, are performed by a CaaS provider on behalf of a device via web services APIs. Cryptography as a service has been defined as being “Keyed cryptographic operations, such as encryption and decryption that are performed by a CaaS provider on behalf of a device via web service APIs”. The way that the “as a service” architecture works is through the implementation of HTTP and systems such as REST and SOAP. The overall architecture is extremely similar to Public Key Authorities (PKA) and Certificate Authorities (CA). The cryptographic keys used to perform

these operations are stored within the CaaS provider, so devices do not possess these keys at any time (refer figure 8).

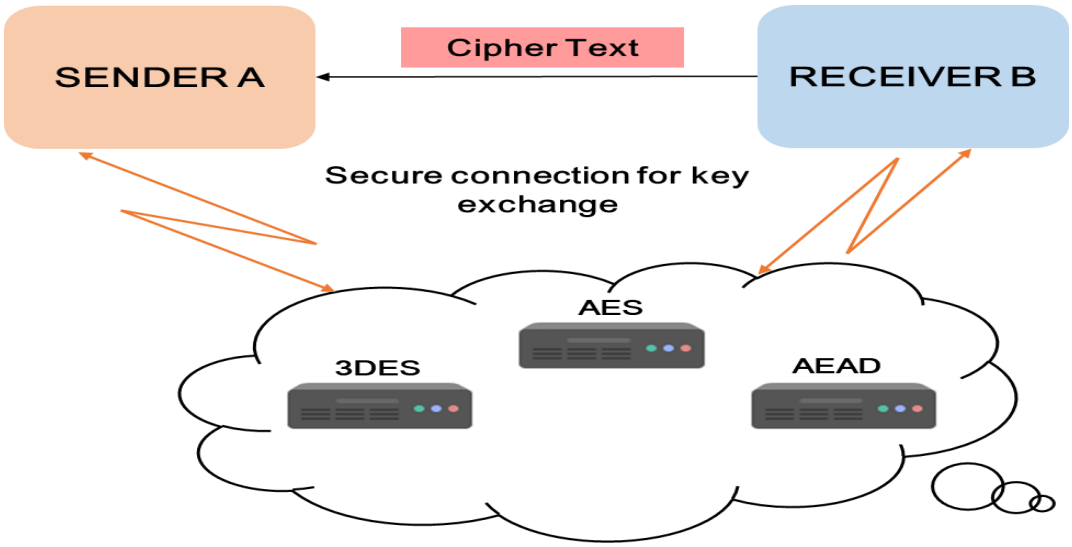

Figure 8: Block Diagram - Cryptography-as-a-Service

2.15.2 Cryptography Service Provider (CSP)

As organisations continue to test and integrate cloud computing into their IT environments, Cryptography-as-a-service and Entropy-as-a-service are into service to safeguard cryptographic keys with the same dynamic and virtualised attributes of cloud computing environments. Additionally, when storing data in multi-clouds, using native encryption from cloud service providers creates silos of data and the risk of not having full control over your keys and data. On-premises Hardware-Secure-Module(HSM) diminish those silos and enable users to know the whereabouts of their keys at all times.

BYOE (bring your encryption), or BYOK (bring your keys), is a security model tailored explicitly to cloud computing. It allows cloud service customers to use their encryption tools and manage their encryption keys.

A cryptographic Service Provider (CSP) allows Cryptographic applications and services to access secure cryptographic operations and Key management. This provider uses the standard REST API, JCE (Java Cryptographic Extension) programming interface. PKCS#11, Cryptography API: Next Generation (CNG), HTTPS, Web API (W3C), Microsoft CAPI, and OpenSSL.

2.15.3 Verification of cloud/service based key lifecycle management

2.15.3.1 Verify integration of Cloud HSM (e.g., AWS Cloud HSM, Azure Key Vault, Google Cloud KMS etc.)

2.15.3.2 All Cloud HSM deployments shall support complete cryptographic key lifecycle management, including secure key generation, storage, usage, rotation, archival, and destruction.

2.15.3.3 Cryptographic keys shall be generated and remain within FIPS 140-2 Level 3 (or higher) validated HSM security boundaries, and plaintext export of key material shall not be permitted from the validated HSM security boundaries.

2.15.3.4 Access to keys shall be governed by role-based access control, enforcing least-privilege, segregation of duties and multi-factor authentication.

2.15.3.5 Key rotation policies shall be mandatorily enforced, with keys rotation periods as per NIST SP 800-57 Part 1 Rev. 5. The key rotation periods shall be shorter for high-risk systems. Longer crypto period is allowed for Root / Master keys but periodic rotation is recommended.

2.15.3.6 Automated rotation mechanisms shall be supported without service disruption, and previous key versions shall remain available for decryption or verification only.

2.15.3.7 All key lifecycle events—including creation, access, rotation, policy changes, and destruction—shall generate immutable audit logs.

2.15.3.8 Audit logs shall be tamper-evident, exportable to external systems with audit log retention periods as defined in alignment with NIST SP 800-57, NIST SP 800-53, ISO/IEC 11770, ISO/IEC 27001, and applicable national regulatory requirements, including CERT-In cyber security directions. For e.g. – The Audit logs may be retained online for a minimum of 400 days, and archived securely for a minimum period of seven years.

2.15.3.9 Cryptographic destruction of keys shall be irreversible and verifiable through audit evidence.

2.15.3.10 Check secure key provisioning, distribution, rotation, archival, and destruction mechanisms as per above steps.

2.15.3.11 Verify that only authorized services or users can access HSM APIs and review IAM policies and role-based access configurations.

2.15.3.12 Perform dynamic tests on key management APIs for:

i. Unauthorized access attempts
ii. Replay attacks and injection vulnerabilities
iii. Improper error handling revealing sensitive info
iv. Data-in-Transit and Data-at-Rest Protection

2.15.3.13 Verify Cloud HSM complies with FIPS/ISO standards (or equivalent) at least FIPS 140-2 Level 3 (or higher) validated HSMs.

CHAPTER 3

3.1 Operational, Interface and Interoperability Requirements

3.1.1 Based on network deployment topologies, the cryptographic system should work in point-to-point/ point-to-multipoint / multipoint-to-multipoint mode.

3.1.2 The cryptographic system shall provide Ethernet payload encryption over a point-to-point network.

3.1.3 It must be possible for an operator to select a particular encryption scheme for payload encryption system wise.

i. It shall provide confidentiality and protection from firmware upgrades.

ii. It shall support Policy based encryption.

iii. It shall provide data protection against unauthorised access by users and processes in physical, virtual, and cloud environments so that implementation is seamless and transparent to application/presentation of layer of system and its storage. So it can work across an enterprise's entire environment.

iv. Regardless of performance level, the cryptographic system shall be interoperable with the appropriate Application interface.

v. It shall provide confidentiality using standard encryption algorithms in a Quantum-safe cryptosystem and applicable algorithms in asymmetric and hash functions as per the product's specification sheet.

3.2 Operational requirements of a cryptographic system

Sl. No.	Parameter Type	Description and range of the Parameters	Reference Standard(s)	Remarks
1.	Traffic type	Unicast / Multicast / Broadcast over IP networks (IPv4 / IPv6)	IPv4: RFC 791, IPv6: RFC 8200	To be confirmed as per applicable RFCs and product scope
2.	No of Concurrent connection	User-to-Server mode: support at least 100/500 connections as applicable	TCP: RFC 9293, TLS 1.3: RFC 8446	Exact value to be finalized by procurer based on deployment sizing; verification via load/concurrency testing
3.	Direction of data transmission	Full duplex	IEEE 802.3 (Ethernet), as applicable	Low overhead bits
4.	Separation of data/control plane	Separation of Control plane and data plane	Product architecture / deployment specification	Physical and logical separation of data and control plane

5.	Latency at specified rate (server/client)	Latency at node (non-aggregation state) ≤ 10 µs for data throughput up to 10 Gb/s	--	Latency requirement to be independent of packet/Ethernet frame size
6.	Support of Jumbo frames	Support Ethernet frames larger than standard MTU; configurable jumbo frame size	IEEE 802.3	Beyond standard ethernet frame size, exact maximum MTU to be specified by procurer
7.	Mode of secure key uploading	Manual/Automatic	ISO/IEC 19790:2025	Applicable according to security level 1/2/3/4
8.	Software/ Firmware loading	The cryptographic module can load software or firmware from an external source.	ISO/IEC 19790:2025 Clause 7.4.3.4	A validation authority shall validate the integrity/authenticity of loaded software or firmware before loading.
9.	Self-test for the	Cryptographic module pre-operational and conditional self-tests	ISO/IEC 19790:2025 Clause 7.10	Conditional self-tests shall be performed when

	integrity of H/W and S/W modules	provide the operator assurance that faults have not been introduced that would prevent the module's correct operation.		an applicable security function or process is invoked.
10.	Module’s version	The cryptographic module shall output the name or module identifier and the versioning information	ISO/IEC 19790:2025 Clause 7.4.3.1	Hardware, software and/or firmware versioning information
11.	Status	The cryptographic module shall output the current status	ISO/IEC 19790:2025 Clause 7.4.3.1	Visual indicators in response to a service request/ normal state
12.	Self-tests	pre-operational self-tests before loaded code can be executed	ISO/IEC 19790:2025 Clause 7.4.3.1	Status shall reflect completion/pass/fail
13.	Approved Security	Approved security	ISO/IEC 19790:2025	at least one test in the approved

	function test	functions	Clause 7.4.3.1	mode of operation
14.	Zeroisation	Perform zeroisation (zeroise all unprotected SSPs and key components within the module at all security levels)	ISO/IEC 19790:2025 Clause 7.4.3.1	Zeroisation shall be immediate and uninterruptable in Security Level 4
15.	Mode of operation	Normal/degraded	ISO/IEC 19790:2025 Clause 7.2.4.3	Normal mode only if all pre-operational self-tests pass
16.	Bypass capability	Indicate whether the Bypass capability is activated or not	ISO/IEC 19790:2025 Clause 7.2.4.3	Bypass allowed only with controls preventing inadvertent plaintext exposure due to a single error
17.	Self-Initiated cryptographic output Test	Indicate capability for self-initiated crypto output test without Crypto Officer configuration;	ISO/IEC 19790:2025	this configuration may be preserved over resetting, rebooting, or power cycling of the module

		show status when enabled		
18.	Operational environment	i. A non-modifiable operational environment ii. A limited operational environment. A modifiable operational environment	ISO/IEC 19790:2025 Clause 7.6	Functions may be added or modified within the operational environment.
19.	Life-cycle assurance	Confirm the best practices by the vendor of a cryptographic module during the design, development, operation and end of life of a cryptographic module.	ISO/IEC 19790:2025 Clause 7.11	Vendor to provide evidence covering defined lifecycle stages
20.	Power	AC supply 110-230V +10% 50/60 Hz AC	Vendor specification	AC or DC supply or both as optional Procurer to specify connector type and

				redundancy if required
21.	DC power	DC supply range: –40 V to –60 V DC (including renewable sources, as applicable)	Vendor specification	
22.	Size	Dimensions in mm or inches in length, width and height	Vendor specification	Desirable: 1U; multiple 1U options acceptable
23.	Cooling	Requirement of Ingress or Egress fans (suck and exhaust kind of setup).	--	Fan may be optional depending on environment; temperature maintenance is mandatory
24.	Min Altitude without any degradation	Normal operation without any degradation at an altitude of upto 3,000 meters.	--	The manufacturer shall guarantee satisfactory performance
25.	Power Supply Alarm	Visual indicator (e.g., Green/Red) for		Indicate the status of power AC/DC.

		AC/DC power status		
26.	Encryption/ De cryption Alarm	Any visual indicator(G/R or any other colour)		To indicate status
27.	Fault Indicator Alarm	Any visual indicator(G/R)	Log message and visual indicator	To indicate status
28.	Capable of functioning in a saline environment	Without any degradation system shall be able to function normally		Self-certificate to be submitted if no test environment is available.

3.3 Interface requirements of a cryptographic system

The cryptographic system shall support 10/100/1000/2500/10000 BASE-TX electrical or optical interface or any open standard port for management as per the user requirement. Hardware/Software of Plaintext Interface shall be physically separate from Hardware/Software of Cipher interface.

Sl. No.	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1.	Management Interface	Optical//Ethernet (RJ45) Ethernet data	ISO/IEC 19790:2025 Clause	i. Applicable interface type(s) depend on module

		input through the command line interface also. SNMP v3 or above, or XML/JSON shall be supported for EMS/NMS/NOC.	7.3.1, 7.3.2	category: ii. (i) HMI (Hardware Module Interface): data port + management port; iii. (ii) SFM (Software/Firmware Module): logical interfaces; iv. (iii) HSMI/HFMI (Hybrid SW/FW Module Interface): plaintext/ciphertext interface separation
2.	Data input interface	Interface (plain text, cipher text and SSP)	ISO/IEC 19790:2025 Clause 7.3.3(a)	
3.	Data output interface	Interface (plain text, cipher text and SSP)	ISO/IEC 19790:2025 Clause 7.3.3(b)	
4.	Control input	All input commands,	ISO/IEC 19790:202	Access control/authentic

	interface	signals, and control data (e.g., clock input, function calls, manual controls such as switches/ buttons/ keyboards)	5 Clause 7.3.3(c)	ation applies as per module security policy
5.	Control output interface	All output command s, signals, and control data	ISO/IEC 19790:202 5 Clause 7.3.3(d)	Inhibited when the cryptographic module is in an error state unless exceptions are specified
6.	Power interface	All external electrical power entering/leaving the cryptographic module (not applicable to pure software-only modules)	ISO/IEC 19790:2025 Clause 7.3.3(g)	Except in the software module, power is provided internally by the source of the battery.
7.	Status output	All status output signals, indicators, and status data (including visual/audio/me	ISO/IEC 19790:2025 Clause 7.3.3(e)	Includes error indicators (return codes), displays/LEDs, buzzer/tone/ring/ vibration where

		chanical indicators)		implemented
8.	Trusted channel (Security Level 3 and above)	Protected link for transmission of unprotected plaintext CSPs/key components and authentication data between module and endpoint	ISO/IEC 19790:2025 Clause 7.3.4	For Security Level 4, multi-factor identity-based authentication shall be employed for all services utilising the trusted channel

3.4 Interoperable requirements of a cryptographic system

Interoperability is one of the essentials to making seamless internetwork function in a heterogeneous network environment. The application service layer in the cryptographic system communicates with the key management controller. Communication protocol and data format for a quantum key distribution (QKD) network or any Key source network to supply cryptographic keys to an application, i.e., a Cryptographic system.

Sl. No.	Name of the Sub parameter	Types of Parameters range	Reference Standard(s)	Remarks
1.	IP Layer	Internet Protocol (IP) IPV4/IP6, Internet Control	IETF RFCs IPv4: RFC 791; IPv6: RFC 8200; ICMPv4: RFC	Confirm interworking for both IPv4 and IPv6;

		Message Protocol (ICMP), Internet Group Management Protocol (IGMP), IPSec	792; ICMPv6: RFC 4443; IGMP: RFC 3376; IPsec: RFC 4301 (and related RFCs)	
2.	Authentication	CA-based authentication and/or AAA-based authentication (as applicable)	X.509/PKI; RADIUS: RFC 2865; TLS: RFC 8446	CA trust model as per (enterprise CA / public CA / local RA); RADIUS server may be used for centralized AAA
3.	Encryption	Various encryption methods as listed	NIST-approved algorithms (as applicable)	Device shall support configured algorithms/cipher suites as per security policy
4.	Key exchange (KMIP)	During a key exchange with other systems	OASIS standard	--
5.	API with QKD interface	REST/HTTPS API for middleware integration; JSON encoding	HTTPS/TLS: RFC 8446; JSON: RFC 8259	--
6.	Inter Secure	Master SAE ↔ Slave SAE	QKD link as per ETSI GS	SAE of cryptographic

	Application Entity (SAE)	communication for QKD key delivery/control	QKD 004	system connects to the QKD KME
7.	SSH	User authentication layer, transport layer, connection layer	RFC 4252, RFC 4253, RFC 4254	SSH may be used in several methodologies like for secure administration/management access
8.	TLS	TLS v1.3 or above	IETF RFC 8446	Use for management/API channels and other interfaces requiring secure transport
9.	Entropy source	Proven/validated randomness source for key generation and nonce	NIST SP standards, TEC QRNG standard	Examples: on-chip TRNG, dedicated circuitry, external entropy source;
10.	Clock	Internal circuit or External I/O timing source	Product/platform spec	Used for control functions, timeouts, scheduling, counters/ ticks; accuracy requirements to be specified if needed

11.	Link layer protocols	L2 options such as Ethernet MAC, PPP, tunneling (as applicable)	IEEE 802.3; PPP: RFC 1661; relevant tunnel RFCs as applicable	Layer 2 protocol communications

Intentionally Left Blank

CHAPTER 4

Security Requirements

4.1 Security services requirements of a cryptographic system

The following security services are required for the enhancement of security;

i. Authentication mechanisms may be needed within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorised to assume the requested role and perform services within that role. The cryptographic system shall support lossless data encryption/ decryption key change.

ii. It should implement a key integrity check and authentication mechanism through a suitable hashing algorithm.

iii. Encryption keys should be encrypted, stored in a secure device and only accessible to the user, regardless of data and key storage methods.

4.2 Security/Assurance level classification and requirements

The cryptographic techniques (algorithms and protocols) may remain the same across different security/assurance levels; however, the assurance requirements increase with the risk category, usage environment, and deployment criticality. Selection of a PQC-based cryptographic solution shall therefore be based on the assurance level appropriate to the application's risk appetite and the operational environment. The hierarchical structure defines that higher assurance implies compliance with lower assurance requirements, and the quantum-safe cryptographic systems are classified into Level 1, Level 2, Level 3, and Level 4 based on security needs and deployment context.

i. **Security/Assurance Level 1:** Provides a baseline level of security for PQC adoption in non-sensitive, consumer-grade environments. Focus is on basic PQC compliance, correctness, interoperability (including RFC conformance where applicable), and basic performance checks. Basic security requirements are specified for a cryptographic module (e.g. at least one approved security function or approved sensitive security parameter establishment method shall be used). Ideally appropriate for security applications where controls, such as physical security, network security, and administrative procedures, are provided outside the module but within the deployable environment.

ii. **Security/Assurance Level 2:** Applies to PQC products/solutions handling sensitive data in consumer-grade environments, including cloud-integrated implementations. Level 2 is additionally bifurcated in three sub Levels – Level 2A (Secure Software Assurance for software based PQC products), Level 2B (Secure Hardware Assurance (IoT/IT) for hardware based IT/IoT products) and Level 2C (Hardware Assurance (OT) for hardware based OT products). In addition to Level 1 checks, it emphasizes secure software assurance such as robustness, fuzz/negative testing, vulnerability assessment, and secure coding practices. It enhances the physical security mechanisms of Security Level 1 by adding the requirement for tamper evidence, including tamper-evident coatings or seals or pick-resistant locks on removable covers or doors. Security Level 2 allows a cryptographic software module to be executed in an adaptable environment that implements role-based access controls or, at the minimum, a discretionary access control with the robust mechanism of defining new groups and assigning restrictive permissions through access control lists (e.g. ACLs), and with the

capability of setting each user to more than one group, and that protects against unauthorised execution, modification, and reading of cryptographic software.

iii. **Security/Assurance Level 3:** Applies to enterprise-grade deployments requiring long-term security for sectors such as finance, telecom, and health. In addition to Level 2 requirements, it introduces stronger enterprise controls such as crypto-agility validation, stronger entropy validation expectations (TRNG/QRNG as applicable), centralized cryptographic management integration, and broader enterprise security assurance practices. It provides additional requirements to mitigate unauthorised access to SSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits. The physical security mechanisms may include solid enclosures and tamper detection/response circuitry that zeroise all CSPs when the removable covers/doors of the cryptographic module are opened. Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorised to assume a specific role and perform a corresponding set of services. Security Level 3 requires manually established plaintext CSPs to be encrypted, utilise a trusted channel or use a split knowledge procedure for entry or output.

iv. **Security/Assurance Level 4:** Applies to sovereign-grade / critical information infrastructure protection. This level represents the most stringent assurance, including the strongest security assurance expectations (e.g., strategic resilience, rigorous supply chain assurance, nation-state attack simulation–type security validation), and strategic sector-specific requirements. The physical security mechanisms provide a complete envelope of protection around the cryptographic module to detect and respond to all unauthorised attempts at physical access when SSPs are contained in the module, whether external power is applied or not. Penetration of the cryptographic module enclosure from any direction is highly likely to be detected, resulting in the immediate zeroisation of all unprotected SSPs. Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At a minimum, this requires two of the following three attributes. At Security Level 4, a cryptographic module is required to include special environmental protection features designed to detect voltage and temperature boundaries and zeroise all unprotected SSPs to provide a reasonable assurance that the module will not be affected when outside of the normal operating range in a manner that can compromise the security of the module.

4.2.1 The product shall meet at least Level 2A for software products and Level 2B (ICT products) or 2C (OT products) for commercial usage (i.e. for Medium Risk usage) and therefore, shall cater to below functional requirements:

4.2.2 The product shall enforce and validate multi-person (M-of-N) authorization controls for all critical cryptographic operations, including master key generation, activation, and destruction. Validation shall confirm that operations cannot be executed without the required quorum, that

minimum M and N values are configurable based on assurance level, and that single-person compromise is technically prevented. All multi-person control events shall be securely logged, auditable, and resistant to bypass or circumvention. The M-of-N quorum shall be mandatorily enforced for any changes to the PQC Transition Policy, including the switching of operating modes from "Hybrid" to "PQC-Only" or "Classical-Only."

4.2.3 The product shall enforce protocol-level protections against PQC parameter downgrade attacks, ensuring that adversaries cannot force negotiation of weaker security parameter sets when stronger options are available. Validation shall demonstrate strict enforcement of minimum approved parameter sets, rejection of downgrade attempts, immutable policy configuration, and conformance testing across supported protocols to ensure downgrade resistance cannot be bypassed.

4.2.4 The OEM shall ensure that Vulnerability Assessment and Penetration Testing (VA/PT) of the system is carried out by a designated security lab by NCCS or Information Security Auditing Organization empanelled with CERT-In (MeitY, Government of India). For the cyber security audits that are conducted, ensure the adherence to latest guidelines issued by CERT-In or issued by Sectoral CERTs. The VA/PT report shall be submitted and reviewed for following:

4.2.4.1 Ensure testing covered all application components — API endpoints, web UI, backend services, and data interfaces.

4.2.4.2 Verify that cloud integrations and HSM interfaces were included in testing.

4.2.4.3 Ensure both automated and manual testing were performed.

4.2.4.4 Review the VA/PT report for:

i. Classification of vulnerabilities (Critical, High, Medium, Low)
ii. Risk rating and CVSS scoring
iii. Recommended mitigations and closure evidence
iv. Mitigation Verification

v. Check that all Critical and High vulnerabilities have been remediated and re-tested.

4.2.4.5 Validate that residual risk is documented and approved.

4.2.4.6 Secure Coding practice shall be verified with steps as under:

4.2.4.7 Static Analysis using tools.

4.2.4.8 Manual code inspection to verify:

i. Input validation and sanitization

ii. Proper authentication and session management

iii. Secure cryptographic implementations (e.g., no hardcoded keys)

iv. Error/exception handling without information leakage

v. Cryptographic Abstraction Layer-Verification shall confirm that all cryptographic functions are called via a standardized Abstraction Layer (API). Direct hard-coding of specific algorithms within application logic shall be prohibited.

4.2.4.9 The limited lists such as OWASP Top 10, SANS Top 25 and similar, should not be considered as standards or references. Instead, discovery of all known vulnerabilities should be based on the comprehensive standards/frameworks.

4.2.4.10 Check for vulnerabilities in third-party libraries

4.2.4.11 Confirm use of version control with restricted access (multi factor authentication)

4.2.4.12 Ensure code commits and merges require peer review and approval.

4.2.4.13 Ensure adherence to latest design/secure coding guidelines issued by CERT-In and applicable Sectoral CERTs.

4.2.4.14 For Hardware Assurance wherever applicable, inspection shall be done to validate Secure element, Trusted Execution Environment (TEE), Physically Unclonable Functions (PUFs), Secure boot attestation and tamper proofness.

4.3 Additional requirements for Level 3 – Enterprise Grade

4.3.1 Quantum/True RNG (QRNG/TRNG) Assurance

4.3.1.1 The product shall integrate QRNG/TRNG compliant with TEC GRs or equivalent globally recognized standards.

4.3.1.2 The QRNG/TRNG shall undergo validation of its claimed physical entropy source (quantum, optical, or other physical mechanisms).

4.3.1.3 The entropy source validation shall demonstrate that the source is genuine, continuously operational, and not simulated or emulated.

4.3.1.4 Validation shall include:

a) Auditable scientific documentation of the entropy mechanism
b) Hardware BoM verification of entropy source components
c) Calibrated test evidence demonstrating entropy generation
d) Continuous health monitoring of the entropy source

4.3.1.5 The QRNG/TRNG shall ensure that the entropy source cannot be spoofed, substituted, or disabled without detection.

4.3.1.6 Calibration certificates for entropy sources shall be maintained and provided as validation evidence.

4.3.1.7 The product shall ensure non-repudiation, integrity, and non-repetition of entropy-derived seed material across sessions, restarts, and lifecycle events.

4.4 Performance and Resource Monitoring

4.4.1 The product shall support measurement and reporting of memory utilization (heap/stack) and binary footprint for all cryptographic implementations.

4.4.2 The product shall record CPU/GPU utilization during cryptographic operations including encapsulation/decapsulation and signature generation/verification.

4.4.3 The product shall measure power consumption under idle, average, and peak workloads and compute energy per cryptographic operation.

4.4.4 The product shall support scalability validation through concurrent cryptographic sessions under mixed workloads.

4.4.5 The product shall enable packet-level analysis to assess bandwidth overhead, link utilization, and QoS under encrypted traffic conditions.

4.4.6 Performance benchmarks shall be configurable based on sector-specific requirements.

4.5 Crypto-Agility

4.5.1 The product shall support switching between classical, hybrid, and PQC algorithms through CLI, GUI, or API interfaces.

4.5.2 Cryptographic switching shall occur without system reboot and with minimal service disruption as per defined SLA requirements.

4.5.3 The product shall support fallback to classical cryptography in case of PQC module failure, disablement, or overload without data loss.

4.5.4 The product shall support seamless rollback to previously validated cryptographic configurations.

4.5.5 The product shall support integration of new cryptographic algorithms through firmware or software updates.

4.5.6 The product shall include a documented cryptographic transition and upgrade policy.

4.6 Security Validation and Assessment

4.6.1 The product shall undergo protocol-level security validation through advanced attack simulations including fault injection and multi-vector attacks.

4.6.2 The product shall support automated vulnerability discovery and formal security analysis.

4.6.3 Security audit and assessment reports shall be maintained and made available.

4.7 Key Derivation and Cryptographic Integration

4.7.1 The product shall derive final encryption keys using a secure Key Derivation Function (KDF).

4.7.2 The KDF shall securely combine all applicable entropy sources including PQC outputs, QRNG seeds, and QKD-derived keys (where applicable).

4.7.3 The product shall support secure integration with centralized cryptographic management systems.

4.7.4 The integration shall ensure secure communication, authenticated access, and authorized management control.

4.7.5 The product shall support reporting of cryptographic inventory, algorithm status, versions, and health metrics.

4.7.6 Supported management protocols (e.g., SNMP, REST APIs) shall be documented and validated for confidentiality and integrity.

4.8 CI/CD and Regression Validation

4.8.1 The product shall support integration with CI/CD pipelines for automated regression testing.

4.8.2 The CI/CD pipeline shall trigger validation upon code, configuration, or cryptographic changes.

4.8.3 Automated testing shall include unit, integration, security, and interoperability tests.

4.8.4 Builds failing defined quality or security criteria shall not be promoted.

4.8.5 Test results and security findings shall be traceable and retained for audit purposes.

4.8.6 The CI/CD process shall support repeatable builds, version control, and rollback capability.

4.8.7 The product shall support validation across multiple platforms (e.g., Linux, Windows, ARM-based systems).

4.9 Supply Chain and Compliance

4.9.1 The product shall ensure supply chain security across hardware, firmware, software, and critical components.

4.9.2 The vendor shall support compliance with sector-specific cryptographic policies as notified by regulators.

4.10 Additional requirements for Level 4 – Critical Infrastructure Security

4.10.1 Indigenous and Customized Cryptography

The product shall support validation of customized or indigenous cryptographic implementations – *not covered in this GR.*

4.10.2 Strategic Cryptographic Resilience

4.10.2.1 The product shall support rapid cryptographic transition in case of algorithm compromise.

4.10.2.2 The product shall support transition to alternative PQC algorithms or QKD within defined time limits without loss of security.

4.10.2.3 The product shall support pre-configured fallback mechanisms and validated transition procedures.

4.10.2.4 The product shall support algorithm diversification, hybrid models, and multiple trust anchors.

4.10.3 QKD Integration

The product shall support QKD integration readiness as per TEC GRs or equivalent standards.

4.10.4 Fail-Secure Behavior

The product shall ensure fail-secure operation under cryptographic and system failure and shall not fail open under any failure condition.

4.10.5 Disaster Recovery and Business Continuity

The product shall support Disaster Recovery (DR) and Business Continuity (BC). The product shall support multi-site deployment with

secure state consistency. The product shall meet defined RTO and RPO requirements. The product shall support validated failover and failback mechanisms. DR testing shall include simulated failures ensuring no data loss or key compromise.

4.10.6 **Zero Trust Architecture**

The product shall comply with Zero Trust Architecture principles including continuous authentication and authorization.

4.10.7 **Red Teaming and Advanced Threat Validation**

The product shall undergo independent red team testing simulating real-world attacks. Findings shall be documented, risk-rated, remediated, and revalidated.

4.10.8 **Advanced Supply Chain Assurance**

The product shall support semi-formal verification of component provenance and integrity. Critical security components shall undergo semi-formal verification for correctness and vulnerability absence. Verification scope and limitations shall be documented.

4.10.9 **Nation-State Threat Evaluation**

The product shall be evaluated against advanced persistent threat scenarios including supply chain and cryptographic attacks.

4.10.10 **Sector-Specific Extensions**

Additional requirements may be defined by strategic sectors and shall be treated as extensions to this framework.

Intentionally Left Blank

CHAPTER 5

Quality, Safety, EMI/EMC and General Requirements

5.1 Quality requirements of a cryptographic system

5.1.1 The manufacturer shall furnish the MTBF values. A minimum value of MTBF shall be 10,000 hours. The calculations shall be based on the guidelines specified in the standard.

5.1.2 The product/systems shall be manufactured by the international quality management system ISO 9001:2015, for which the manufacturer should be duly accredited. A quality plan describing the manufacturer's quality assurance system must be submitted.

5.1.3 The product/systems shall conform to the requirements for the environment specified in document QM 333 {TEC 14016:2010}: " Standard for environmental testing of Telecommunication Equipment" The applicable tests shall be for environmental category B2, including vibration test.

Quality requirements of a cryptographic system

Sl. No	Name of the Sub parameter	Description of Parameters and its Range	Reference Standard (s)	Remarks
1	Operating Temperature	0°C to +60°C	IEC/ISO	For defence and space requirements to be met as per user specs.
2	Humidity	10 to 90% RH	IEC/ISO	

3	Reliability	Availability / operational uptime expressed as a percentage (e.g., ≥ 99.0%, 99.9%, 99.99%)	--	To be defined by procurer
4	Basic environmental Test	Environmental category B2	QM-333	
5	MTBF (as per BSNL QM-115)	Metric		At least 100,00 hours
6	MTTR	Metric		To be defined by procurer
7	Manufactured process compliance	International quality management	ISO 9001:2015	

5.2 EMI/EMC Requirements of a cryptographic system

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. An accredited test agency shall furnish a test certificate and test report.

a) **Conducted and radiated emission:**

Name of EMC Standard: “CISPR 32: 2015 + A1: 2019- Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits: -

i. To comply with Class B limits of CISPR 32:2015+A1:2019

ii. For Radiated Emission tests, limits below 1 GHz shall be as per relevant limits for measuring the distance of 10m and as per relevant limits for measuring the distance of 3m.

b) **Immunity to Electrostatic discharge (ESD):**

Name of EMC Standard: IEC 61000-4-2 {2025) "Testing and measurement techniques of Electrostatic discharge immunity test". Latest version is of 2025: Performance criteria and Applicable Performance Criteria requirements shall be mentioned as per standard practice.

Limits: -

i. Contact discharge level 2 {± 4 kV} or higher voltage;
ii. Air discharge level 3 {± 8 kV} or higher voltage;

c) **Immunity to radiated RF:**

Name of EMC Standard: IEC 61000-4-3 (2020) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".

Limits: -

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i. Under Test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and
ii. Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.
iii. For Telecom Terminal Equipment without Voice Interfaces
iv. Under Test Level 2 (Test field strength of 3 V/m) for general purposes over 80 MHz–1000 MHz, and for protection

against digital radio telephones and other RF devices over 800 MHz–960 MHz and 1.4 GHz–6.0 GHz.

Latest version is of 2020: Performance criteria and Applicable Performance Criteria requirements shall be mentioned as per standard practice.

d) **Immunity to fast transients (burst):**

Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".

Limits: -

Test Level 2, i.e.,

i. 1 kV for AC/DC power lines;
ii. 0. 5 kV for signal/control/ data/telecom lines;

e) **Immunity to surges:**

Name of EMC Standard: IEC 61000-4-5:2014+A1:2017 “Testing & Measurement techniques for Surge immunity test".

Limits: -

i. For mains power input ports: (a)2 kV peak open circuit voltage for line-to-ground coupling (b) 1 kV peak open circuit voltage for a line-to-line coupling
ii. For telecom ports: (a) Peak open-circuit voltage of 2 kV, line-to-ground
iii. (b) Peak open-circuit voltage of 2 kV for line-to-line coupling

Latest version is of 2017: Performance criteria and Applicable Performance Criteria requirements shall be mentioned as per standard practice.

f) **Immunity to conducted disturbance induced by Radiofrequency fields:**

Name of EMC Standard: IEC 61000-4-6 (2013) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields".

Limits: -

i. Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) **Immunity to voltage dips & short interruptions (applicable to AC mains power input ports, if any):**

Name of EMC Standard: IEC 61000-4-11(2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests".

Limits: -

i. A voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70 % supply voltage for 500ms)

ii. A voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e., 40% supply voltage for 200ms)

iii. A voltage interruption corresponds to a reduction of a supply voltage of > 95% for 5s.

iv. A voltage interruption corresponds to a reduction of a supply voltage of >95% for 10s.

h) **Immunity to voltage dips & short interruptions (applicable to DC mains power input ports, if any):**

Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement

techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.

Limits: -

i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.

ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.

iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.

iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C.

v. Voltage variations corresponding to 80% and 120% of supply for 100 ms to 10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus that satisfies the class B disturbance Limits. Class B is intended primarily for use in the domestic environment and may include the following:

i. Equipment with no fixed place of use; for example, portable equipment powered by built-in batteries;

ii. Telecommunication terminal equipment powered by the telecommunication networks

iii. Personal computers and auxiliary connected equipment

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment that satisfies the class A limits but not the class B limits.

Note 2: The testing agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall follow TEC Standard No. TEC 11016:2016 (TEC/SD/DD/EMC-221/05/OCT-16) and the references mentioned therein unless otherwise specified. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per the above mentioned sub clauses (a) to (h) and TEC Standard No. TEC 11016:2016 (earlier no. TEC/SD/DD/EMC-221/05/OCT-16).

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 32	EN 55032
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11
IEC 61000-4-29	EN 61000-4-29

5.3 Safety Requirements of a cryptographic system

5.3.1 Electrical safety

The equipment shall conform to IS/IEC 62368-1:2023 “Audio/video, information and communication technology equipment as prescribed under Table no. 1 of the TEC document ‘SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT”: TEC10009: 2024”. In case remote line powering is applied, it should comply with [ITU-T K.50], [ITU-T K.51] and [IEC 60950-21]. The safe working practices described in [ITU-T K.64] should be followed when work is carried out outside plant electronic equipment.

5.3.2 Laser safety

Laser safety: The equipment shall conform to IEC 60825-2:2021 for products emitting laser radiation as prescribed under Table no. 1 of the TEC document ‘SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT”: TEC10009: 2024”.

Note: *This test shall be applicable if laser components are directly mounted in the box.*

5.3.3 General Requirements

5.3.3.1 The system shall support In-field firmware upgrades from time to time for a continuation of functionality with the advancement of technology and interoperable and supporting systems to make it compatible.

5.3.3.2 It shall support remote system Software/Firmware upgrades.

5.3.3.3 As and when software bugs are found/ determined, the Manufacturer shall provide patches/firmware replacement, if involved, as mutually agreed between the Purchaser of the instrument and supplier. Modified documentation, wherever applicable, shall also be supplied.

5.3.3.4 The manufacturer/supplier shall furnish the list of recommended spares.

5.3.3.5 The supplier shall have a maintenance/repair facility in India. The supplier shall furnish MTBF and MTTR values.

5.3.3.6 The accessories cables shall have a low attenuation cable link, either optical or Ethernet cable of the latest. The vendor will submit the Specification for the same.

5.3.3.7 It must be possible for an operator to select a particular encryption scheme for payload encryption system wide.

5.3.3.8 It shall automatically exchange a new session key on a pre-set interval of 1-60 minutes or user configured.

5.3.3.9 The new session key shall be generated automatically by a True Random Number Generator (TRNG) or a Pseudo Random Number Generator (PRNG). QRNGs are preferred over other TRNGs and PRNGs.

5.3.3.10 These devices should support high entropy throughput with very high randomness (entropy)

5.3.3.11 It shall provide confidentiality-protected firmware/software upgrades.

5.3.3.12 The encryption devices should be future-proof and fully reprogrammable for an upgrade to new algorithms based on the user requirements or availability of technology from time to time.

5.3.3.13 Cryptographic system can also support Quantum-safe key exchange algorithms under the standardisation process of NIST, along with classical algorithms in a hybrid manner.

5.3.3.14 Remote management should be possible only through secure Management software with minimum 2-factor authentication with hardware binding.

5.3.3.15 Cryptographic system shall support SNMPv3 or the latest and shall provide multiple manager support.

5.3.3.16 Cryptographic system shall support audit and event logging with Syslog support.

5.3.3.17 Cryptographic system shall be able to work with the NTP server for time synchronisation.

5.3.3.18 Cryptographic system shall be able to work with RADIUS or TACAS+ server for authentication.

5.3.3.19 Repair procedure;

i. List of replaceable parts used to include their sources and the approving authority.

ii. Detailed ordering information for all the replaceable parts shall be listed in the manual to facilitate the reordering of spares as and when required.

iii. A systematic procedure for troubleshooting and sub-assembly replacement shall be provided. Test fixtures and accessories required for repair shall also be indicated.

iv. Systematic troubleshooting procedures shall be given for the probable faults with their remedial actions.

Note: The Purchaser may mention the repair manual requirement at the time of ordering.

5.3.3.20 Technical literature in Hindi or English of the instrument with block schematic diagrams shall be provided. The complete layout and circuit diagrams of various assemblies with test voltages and waveforms at different test points of the units shall be provided, wherever required. All aspects of installation, operation, maintenance and repair shall be covered in the manuals. It is suggested that both the Soft copy / QR code and Hard copy to be provided. Soft copy shall be provided both in English and Hindi. The manual shall include the following two parts:

i. Installation, operation and maintenance manual.

ii. Safety measures to be observed in handling the equipment.

iii. Precautions for setting up, measurements and maintenance

iv. Product/equipment required for routine maintenance and calibration, including their procedures.

v. Illustration of internal and external mechanical parts.

vi. A detailed description of the operation of the software used in the equipment, including its installation, loading and debugging etc.

5.3.3.21 Identification of Equipment

i. Equipment shall be marked with the supplier's or Manufacturer's logo/name.

ii. The Model No., serial No., The month and year of manufacture shall be indicated by screen printing on the body of the equipment or by a tamper-proof sticker pasted on the body of the equipment.

iii. Power Supply requirements shall be indicated on the body.

iv. The above markings shall be legible, indelible and easily visible.

Intentionally Left Blank

CHAPTER 6

6.1 Information for the procurer of the product

6.1.1 The procurer should require the vendor to submit Bill of Materials (BOM). The BOM submitted by the vendor should be in adherence to the SBOM, CBOM and HBOM guidelines issued by CERT-In or other sectoral CERTs.

6.1.2 The procurer should require the vendor to demonstrate cryptographic agility as an operational capability and not merely as design intent. The vendor shall provide documented procedures for algorithm addition, replacement, and deprecation without system downtime or architectural redesign.

6.1.3 The procurer should clearly specify acceptable cryptographic assurance mechanisms, such as compliance with ISO/IEC 19790, ISO/IEC 24759, FIPS 140-3, or Common Criteria.

6.1.4 The procurer should require that cryptographic policies (algorithm selection, key sizes, protocol versions) be configurable by the procuring entity and protected against unauthorized modification.

6.1.5 During migration phases, the procurer should mandate support for hybrid cryptographic modes (classical + PQC) with explicit controls to prevent downgrade attacks.

6.1.6 The procurer should require the vendor to disclose the performance, latency, power, and resource impact of post-quantum and hybrid cryptographic mechanisms under expected load conditions.

6.1.7 The procurer should define minimum support and maintenance periods for cryptographic components, including guaranteed availability of security updates until system end-of-life.

6.1.8 The applicability of clauses of GR as per product security Level is also tabulated as under-

GR Chapters	Security/Assurance Levels			
	Level 1	Level 2 (2A, 2B & 2C)	Level 3	Level 4
CH-1 Introduction	No test requirements mentioned, Chapter cover introduction of classical and post quantum algorithms with introduction of cryptographic modules			
Ch-2 - Functional requirements – covers Core cryptographic modules, Protocol/Application Layer Requirements, Crypto agility, Requirements for constrained devices and Cryptography –as –a-service.	Applicable to all levels			
Chapter -3 Operational, Interface and Interoperability Requirements – covers details about interface of product, general description of product like throughput, latency etc. and interoperability requirements like IPv4/IPv6 etc.	Applicable to all levels			
Chapter 4 – Security Requirements	--	Testing as per clause 4.3.	Additional as per clause 4.4	Additional as per clause 4.5
Chapter 5- Quality, Safety, EMI/EMC and General Requirements	Applicable to all levels			

6.2 The below clauses from above chapters of GR are to be decided by procurer.

Sl. No.	GR clause / location (as written in draft)	What the procurer must decide
1.	Ch-3 Operational requirements table – “No of Concurrent connection”	Concurrency capacity sizing
2.	Ch-3 Operational requirements table – “Support of Jumbo frames”	Jumbo frame MTU requirement
3.	Ch-3 Power table – AC supply connector type & redundancy	Power feed and redundancy
4.	Ch-3 Interoperability table – Clock accuracy	Time/clock requirements
5.	Ch-5 Quality requirements table – “Reliability (Availability/uptime)”	Minimum availability target
6.	Ch-5 Quality requirements table – “MTTR”	Maximum MTTR target
7.	Ch-5 General requirements – patch/firmware replacement (“…as mutually agreed between the Purchaser… and supplier”)	Patch/SW update SLA and process
8.	Ch-5 General requirements – Supported encryption/hashing/signature algorithms	Required algorithm/cipher-suite
9.	Ch-5 General requirements – Session key change interval (“pre-set interval 1–60 minutes or user configured”)	Rekey interval policy

10.	Ch-5 General requirements – RNG preference (“QRNGs/TRNG”)	Required entropy source assurance
11.	Ch-5 Repair manual note (“Purchaser may mention the repair manual requirement at the time of ordering”)	Whether repair manual is required

ABBREVIATIONS

For this document the following abbreviations apply:

AC	Alternating Current
ACL	Access Control List
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AH	Authentication Header
ANS	American National Standard
ANSI	American National Standard Institute
CA	Certificate Authority
CBC	Cipher-Block Chaining
CFB	Cipher FeedBack mode
CLI	Command Line Interface
CMAC	Cipher-based Message Authentication Code
CNG	Cryptography API: Next Generation
CSR	Certificate Signing Requests
CTR	Counter
DC	Direct Current
DH	Diffie-Hellmen
DHKE	Diffie-Hellman Key Exchange
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI	electromagnetic Interference
EMC	Electromagnetic compatibility
ESP	Encapsulating Security Payload
FPGA	Field Programmable Gate Array

FTP	File Transfer Protocol
GCM	Galois/Counter Mode
HFE	Hidden Field Equations
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
ITU	International Telecommunication Union
IV	Initialisation Vector
KMAC	Keccak Message Authentication Code
KME	Key Management Entity
KMF	Key Management Framework
KMIE	Key Management Interoperability Protocol
LWE	Learning With Error
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OFB	Output FeedBack mode
OID	Object Identifier
OSI	Open Systems Interconnection
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRNG	Pseudo Random Number Generator
QKD	Quantum Key Distribution

QKDE	Quantum Key Distribution Entity
RADIUS	Remote Authentication Dial-In User Service
REST	REpresentational State Transfer
RH	Relative Humidity
RFC	Request For Comment
RSA	Rivest, Shamir and Adleman
SA	Security Associations
SAE	Secure Application Entity
SIS	Short Integer Solution
SFP	Small Form-factor Pluggable
S/MIME	Secure/Multipurpose Internet Mail Extention
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Sockets Layer
SVP	Shortest Vector Problem
TLS	Transport Layer Security
TRNG	True Random Number Generator
TACAS	Terminal Access Controller Access Control System
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XMSS	eXtended Merkle Signature Scheme

======End of the document ======